SIMBa
Seminari Informal
de Matemàtiques de Barcelona

UNIVERSITAT DE BARCELONA

B:KC Barcelona Knowledge Campus

Seminari Informal de Matemàtiques de Barcelona

***Speaker*:** Sergi Rovira Cisterna.
University: Universitat de Barcelona.

Date: Wednesday, 24th of October.
Schedule: 12:00, *coffee break*; 12:20, talk.
Place: B1 classroom, *Facultat de Matemàtiques* of UB.
Language: English.

Title: An Introduction to post-quantum cryptography.

Abstract: Quantum Computers exploit quantum mechanical phenomena to solve mathematical problems considered difficult or intractable for conventional computers. Ongoing advances in physics point towards the eventual construction of large-scale quantum computers. If these computers are ever build, this would compromise the confidentiality and integrity of our current digital communications.

Post-Quantum Cryptography studies cryptosystems that can be implemented in a classical computer but for which no efficient cryptanalytic technique using either classical or quantum computers is known.

The goal of this talk is to give a broad overview of the field of Post-Quantum Cryptography and present one cryptosystem believed to be post-quantum. All the necessary notions of classical cryptography will be introduced during the talk.

Qui som? El SIMBa és un seminari jove organitzat pels estudiants de doctorat de les Facultats de Matemàtiques i Informàtica de Barcelona. Està dirigit a estudiants de doctorat, de màster i, fins i tot, dels darrers cursos de grau. El nostre objectiu és donar a conèixer la recerca que estem fent, així com adquirir coneixements d'altres àrees de les matemàtiques diferents de les pròpies.

Més informació a `www.ub.edu/simba`.

Si teniu qualsevol dubte o suggeriment podeu posar-vos en contacte amb nosaltres a partir del correu ***seminari.simba@ub.edu***.